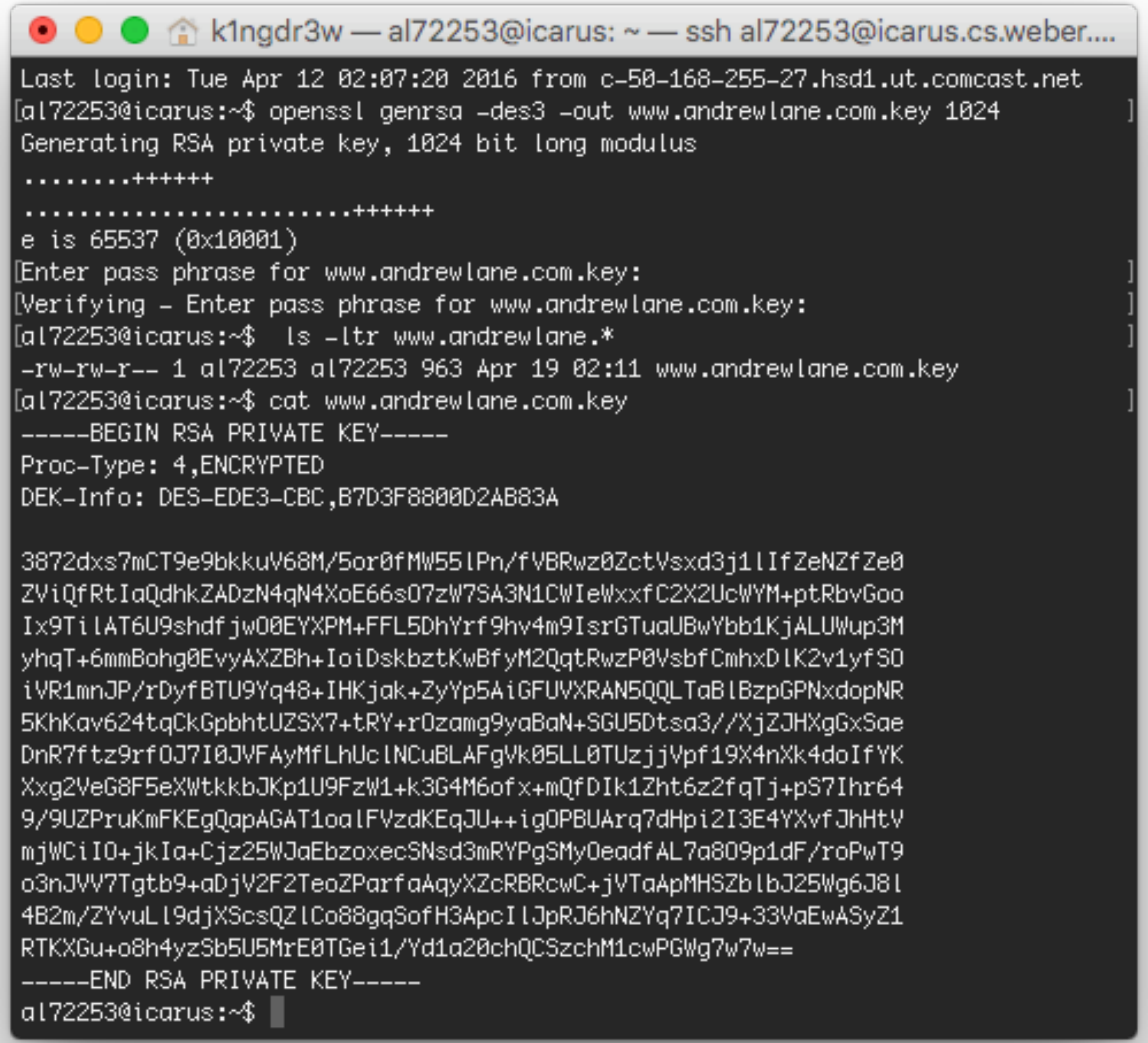
Andrew Lane
4/17/2016
CS2705

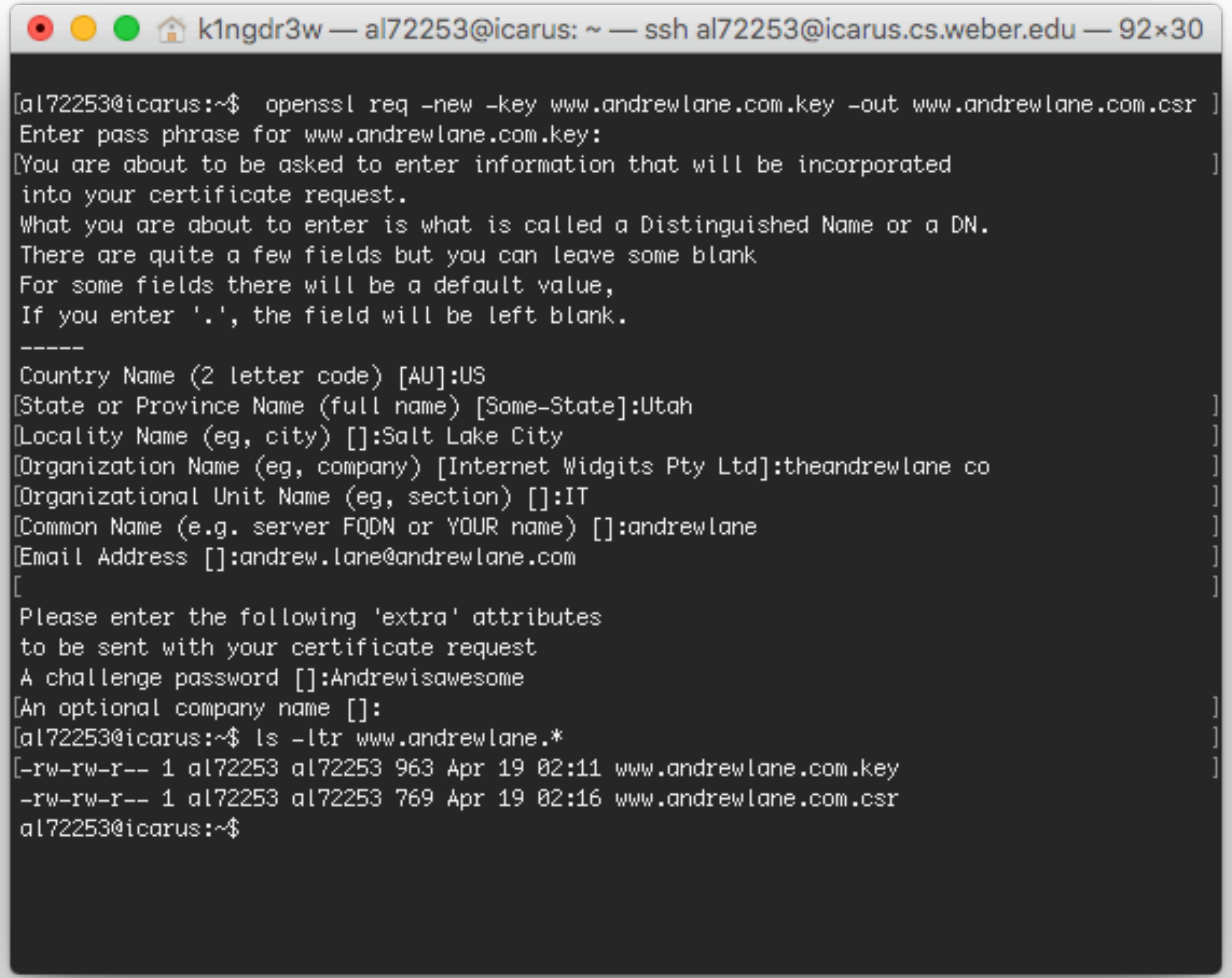
Certificate Lab

1. Here I am generating the initial key for www.andrewlane.com via openssl on the Icarus Linux server.


k1ngdr3w — al72253@icarus: ~ — ssh al72253@icarus.cs.weber....

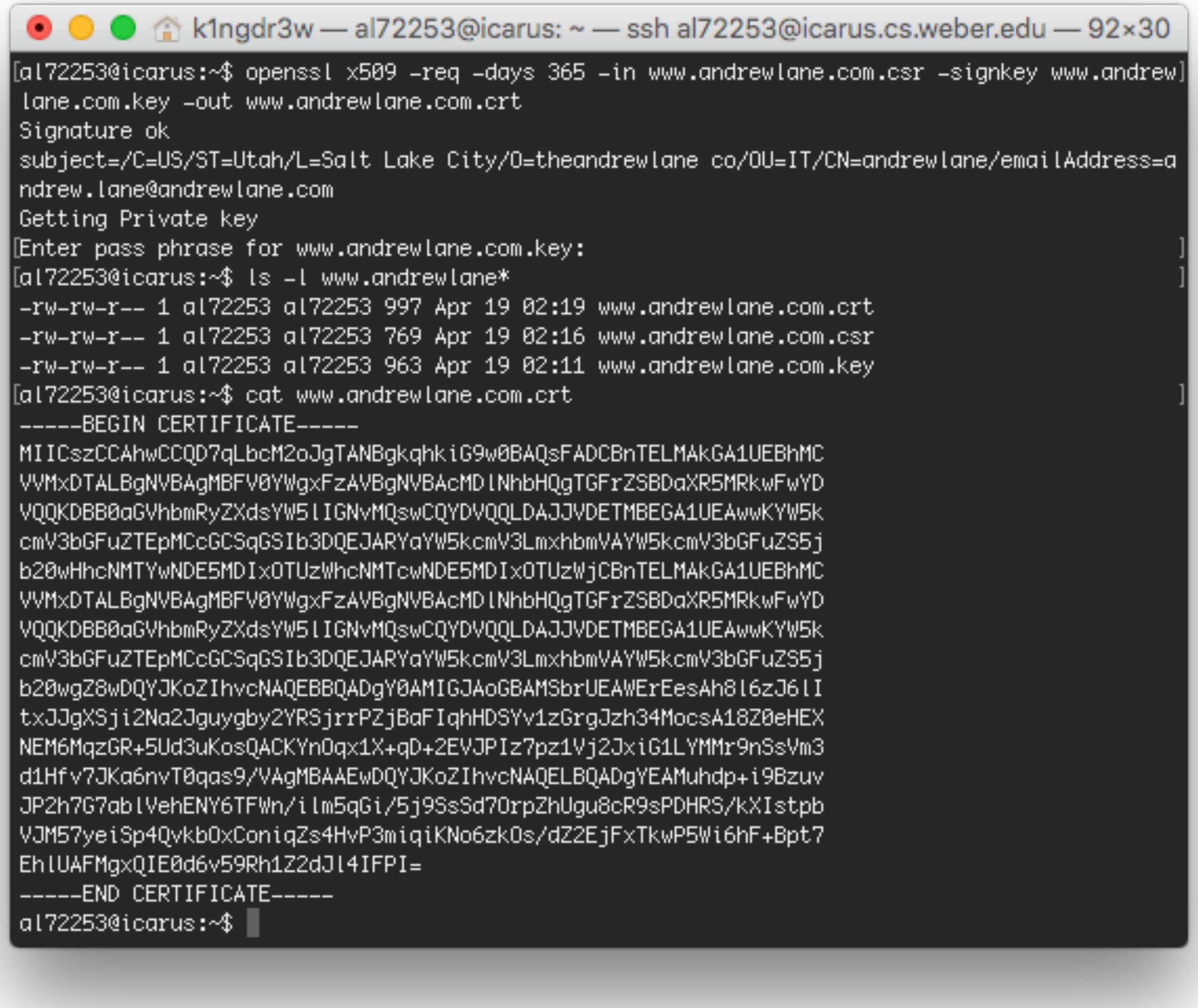
```
Last login: Tue Apr 12 02:07:20 2016 from c-50-168-255-27.hsd1.ut.comcast.net
[al72253@icarus:~$ openssl genrsa -des3 -out www.andrewlane.com.key 1024
Generating RSA private key, 1024 bit long modulus
........++++++
........................++++++
e is 65537 (0x10001)
[Enter pass phrase for www.andrewlane.com.key:
[Verifying - Enter pass phrase for www.andrewlane.com.key:
[al72253@icarus:~$  ls -ltr www.andrewlane.*
-rw-rw-r-- 1 al72253 al72253 963 Apr 19 02:11 www.andrewlane.com.key
[al72253@icarus:~$ cat www.andrewlane.com.key
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,B7D3F8800D2AB83A

3872dxs7mCT9e9bkkuV68M/5or0fMW55lPn/fVBRwz0ZctVsxd3j1lIfZeNZfZe0
ZViQfRtIaQdhkZADzN4qN4XoE66sO7zW7SA3N1CWIeWxxfC2X2UcWYM+ptRbvGoo
Ix9TilAT6U9shdfjwO0EYXPM+FFL5DhYrf9hv4m9IsrGTuaUBwYbb1KjALUWup3M
yhqT+6mmBohg0EvyAXZBh+IoiDskbztKwBfyM2QqtRwzP0VsbfCmhxDlK2v1yfSO
iVR1mnJP/rDyfBTU9Yq48+IHKjak+ZyYp5AiGFUVXRAN5QQLTaBlBzpGPNxdopNR
5KhKav624tqCkGpbhtUZSX7+tRY+rOzamg9yaBaN+SGU5Dtsa3//XjZJHXgGxSae
DnR7ftz9rfOJ7I0JVFAyMfLhUclNCuBLAFgVk05LL0TUzjjVpf19X4nXk4doIfYK
Xxg2VeG8F5eXWtkkbJKp1U9FzW1+k3G4M6ofx+mQfDIk1Zht6z2fqTj+pS7Ihr64
9/9UZPruKmFKEgQapAGAT1oalFVzdKEqJU++igOPBUArq7dHpi2I3E4YXvfJhHtV
mjWCiIO+jkIa+Cjz25WJaEbzoxecSNsd3mRYPgSMyOeadfAL7a8O9p1dF/roPwT9
o3nJVV7Tgtb9+aDjV2F2TeoZParfaAqyXZcRBRcwC+jVTaApMHSZblbJ25Wg6J8l
4B2m/ZYvuLl9djXScsQZlCo88gqSofH3ApcIlJpRJ6hNZYq7ICJ9+33VaEwASyZ1
RTKXGu+o8h4yzSb5U5MrE0TGei1/Yd1a20chQCSzchM1cwPGWg7w7w==
-----END RSA PRIVATE KEY-----
al72253@icarus:~$
```

2. Here I’m generating the certificate signing request, or CSR. This process requires that I use a key, and I will be using the RSA private key generated in the above step. The CSR contains information related to www.andrewlane.com, not all parameters were used here because they were not all required.


k1ngdr3w — al72253@icarus: ~ — ssh al72253@icarus.cs.weber.edu — 92×30

```
[al72253@icarus:~$  openssl req -new -key www.andrewlane.com.key -out www.andrewlane.com.csr ]
 Enter pass phrase for www.andrewlane.com.key:
[You are about to be asked to enter information that will be incorporated                  ]
 into your certificate request.
 What you are about to enter is what is called a Distinguished Name or a DN.
 There are quite a few fields but you can leave some blank
 For some fields there will be a default value,
 If you enter '.', the field will be left blank.
 -----
 Country Name (2 letter code) [AU]:US
[State or Province Name (full name) [Some-State]:Utah                                      ]
[Locality Name (eg, city) []:Salt Lake City                                                ]
[Organization Name (eg, company) [Internet Widgits Pty Ltd]:theandrewlane co               ]
[Organizational Unit Name (eg, section) []:IT                                              ]
[Common Name (e.g. server FQDN or YOUR name) []:andrewlane                                 ]
[Email Address []:andrew.lane@andrewlane.com                                               ]
[                                                                                          ]
 Please enter the following 'extra' attributes
 to be sent with your certificate request
 A challenge password []:Andrewisawesome
[An optional company name []:                                                              ]
[al72253@icarus:~$ ls -ltr www.andrewlane.*                                                ]
[-rw-rw-r-- 1 al72253 al72253 963 Apr 19 02:11 www.andrewlane.com.key                      ]
 -rw-rw-r-- 1 al72253 al72253 769 Apr 19 02:16 www.andrewlane.com.csr
 al72253@icarus:~$
```

3. Finally, in this step I’m generating the self-signed SSL certificate (CRT) via openssl. This certificate is valid for 365 days and requires both the CSR and key generated in the previous steps.



k1ngdr3w — al72253@icarus: ~ — ssh al72253@icarus.cs.weber.edu — 92×30

```
[al72253@icarus:~$ openssl x509 -req -days 365 -in www.andrewlane.com.csr -signkey www.andrew]
 lane.com.key -out www.andrewlane.com.crt
 Signature ok
 subject=/C=US/ST=Utah/L=Salt Lake City/O=theandrewlane co/OU=IT/CN=andrewlane/emailAddress=a
 ndrew.lane@andrewlane.com
 Getting Private key
[Enter pass phrase for www.andrewlane.com.key:
[al72253@icarus:~$ ls -l www.andrewlane*
 -rw-rw-r-- 1 al72253 al72253 997 Apr 19 02:19 www.andrewlane.com.crt
 -rw-rw-r-- 1 al72253 al72253 769 Apr 19 02:16 www.andrewlane.com.csr
 -rw-rw-r-- 1 al72253 al72253 963 Apr 19 02:11 www.andrewlane.com.key
[al72253@icarus:~$ cat www.andrewlane.com.crt
 -----BEGIN CERTIFICATE-----
 MIICszCCAhwCCQD7qLbcM2oJgTANBgkqhkiG9w0BAQsFADCBnTELMAkGA1UEBhMC
 VVMxDTALBgNVBAgMBFV0YWgxFzAVBgNVBAcMDlNhbHQgTGFrZSBDaXR5MRkwFwYD
 VQQKDBB0aGVhbmRyZXdsYW5lIGNvMQswCQYDVQQLDAJJVDETMBEGA1UEAwwKYW5k
 cmV3bGFuZTEpMCcGCSqGSIb3DQEJARYaYW5kcmV3LmxhbmVAYW5kcmV3bGFuZS5j
 b20wHhcNMTYwNDE5MDIxOTUzWhcNMTcwNDE5MDIxOTUzWjCBnTELMAkGA1UEBhMC
 VVMxDTALBgNVBAgMBFV0YWgxFzAVBgNVBAcMDlNhbHQgTGFrZSBDaXR5MRkwFwYD
 VQQKDBB0aGVhbmRyZXdsYW5lIGNvMQswCQYDVQQLDAJJVDETMBEGA1UEAwwKYW5k
 cmV3bGFuZTEpMCcGCSqGSIb3DQEJARYaYW5kcmV3LmxhbmVAYW5kcmV3bGFuZS5j
 b20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMSbrUEAWErEesAh8l6zJ6lI
 txJJgXSji2Na2Jguygby2YRSjrrPZjBaFIqhHDSYv1zGrgJzh34MocsA18Z0eHEX
 NEM6MqzGR+5Ud3uKosQACKYnOqx1X+qD+2EVJPIz7pz1Vj2JxiG1LYMMr9nSsVm3
 d1Hfv7JKa6nvT0qas9/VAgMBAAEwDQYJKoZIhvcNAQELBQADgYEAMuhdp+i9Bzuv
 JP2h7G7ablVehENY6TFWn/ilm5qGi/5j9SsSd7OrpZhUgu8cR9sPDHRS/kXIstpb
 VJM57yeiSp4QvkbOxConiqZs4HvP3miqiKNo6zkOs/dZ2EjFxTkwP5Wi6hF+Bpt7
 EhlUAFMgxQIE0d6v59Rh1Z2dJl4IFPI=
 -----END CERTIFICATE-----
 al72253@icarus:~$
```

That’s it! Now www.andrewlane.com has an SSL certificate. It’s worth noting however that navigating to this public site would bring up a warning in your browser. This certificate is not signed by a valid organization like Verisign or Thawte. However this cert could be used for testing against localhost.